United States District Court

STATE AND DISTRICT OF MINNESOTA

In the Matter of the Search of
(Name, address or brief description of person or property to be searched)

3536 23rd Avenue South, Minneapolis, Minnesota, is described as a two(2) story residential structure that is light in color with yellow trim. When facing the residence from 23rd Avenue South, the numerals "3536" are clearly visible and are affixed to the residence above the front door. The detached garage is white with yellow trim and has a green garage door. When facing the garage door, the numerals "3536" are clearly visible and are affixed to the garage to the left side of the garage door.

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

Case Number:

09-mj-263 JJK

I, Robert J. E. Blackmore, being duly sworn depose and say:

I am a(n) Special Agent, FBI and have reason to believe that ☐ on the person of or ☒ on the premises known as (name, description and/or location)

3536 23rd Avenue South, Minneapolis, Minnesota, is described as a two(2) story residential structure that is light in color with yellow trim. When facing the residence from 23rd Avenue South, the numerals "3536" are clearly visible and are affixed to the residence above the front door. The detached garage is white with yellow trim and has a green garage door. When facing the garage door, the numerals "3536" are clearly visible and are affixed to the garage to the left side of the garage door.

in the State and District of Minnesota there is now concealed a certain person or property, namely (describe the person or property)

Please see Attached List of Items to be Seized.

which is (state one or more bases for search warrant and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

property that constitutes evidence of the commission of a crime, contraband, fruits of criminal activity, and/or means of committing a crime

concerning a violation of Title 18, United States Code, Section(s) 2252.

The facts to support a finding of Probable Cause are as follows:

See Affidavit attached hereto and incorporated herein by reference.

Continued on the attached sheet and made a part hereof. ☒ Yes ☐ No

Signature of Affiant
ROBERT J. E. BLACKMORE, Special Agent
FBI

Sworn to before me, and subscribed in my presence

7/27/09 4:00 pm at St. Paul, MN
Date and Time Issued City and State

The Honorable Jeffrey J. Keyes
UNITED STATES MAGISTRATE JUDGE
Name and Title of Judicial Officer

3

Signature of Judicial Officer

STATE OF MINNESOTA)
) SS. AFFIDAVIT OF ROBERT J. E. BLACKMORE
COUNTY OF RAMSEY)

I, Robert J. E. Blackmore, being duly sworn, hereby depose and say:

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed for over eight years. I am currently assigned to the Minneapolis, Minnesota, Division of the FBI and work on the Minnesota Cyber Crime Task Force. I have received specialized FBI training in both the investigation of computer and computer-related crimes and crimes involving the sexual exploitation of children. As a member of the Cyber Crime Task Force, my responsibilities include the investigation of various criminal offenses involving computers, computer networks, and the Internet, including the investigation of crimes involving the sexual exploitation of children. While employed by the FBI, I have participated in numerous investigations in which I have collected evidence in an electronic form.

2. I am investigating the activities of the Internet account registered to Gregg A. Larsen (Larsen), who resides at 3536 23rd Ave. S., Minneapolis, Minnesota. As will be shown below, there is probable cause to believe that someone using the Internet account registered to Larsen has received, possessed,

or distributed child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. I submit this application and affidavit in support of a search warrant authorizing a search of Larsen's residence, located at 3536 23rd Ave. S., Minneapolis, Minnesota (the "premises"), as further described in Attachments A and B. Located within the premises to be searched, I seek to seize evidence, fruits, and instrumentalities of the forgoing criminal violations, which relate to the knowing transportation, shipment, receipt, possession, distribution, and reproduction of child pornography. I request authority to search the entire premises, including the residential dwelling, detached garage, and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

3. The statements in this affidavit are based in part on information provided by SA J. Brooke Donahue of the Innocent Images Unit of the FBI, located in Calverton, Maryland, other law enforcement officers, and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and

instrumentalities of the violation of §§ 2252 and 2252A, are presently located at 3536 23rd Ave. S., Minneapolis, Minnesota.

STATUTORY AUTHORITY

4. This investigation concerns alleged violations of 18 U.S.C. §§ 2252 and 2252A, relating to material involving the sexual exploitation of minors.

a. 18 U.S.C. § 2252(a)(1) prohibits knowingly transporting or shipping in interstate or foreign commerce, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct.

b. 18 U.S.C. § 2252(a)(2) prohibits knowingly receiving or distributing distribute, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct that has been mailed, shipped, or transported in interstate or foreign commerce. That section also prohibits knowingly reproducing any visual depiction of minors engaging in sexually explicit conduct for distribution in interstate or foreign commerce by any means, including by computer or the mail.

c. 18 U.S.C. § 2252(a)(4) prohibits possessing one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been transported in interstate or foreign commerce, or that were produced using materials that had traveled in interstate or foreign commerce.

d. 18 U.S.C. § 2252A(a)(1) prohibits knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer.

e. 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

f. 18 U.S.C. § 2252A(a)(3)(A) prohibits a person from knowingly reproducing child pornography for distribution through the mail or in interstate or foreign commerce by any means, including by computer.

g. 18 U.S.C. § 2252A(a)(3)(B) prohibits knowingly advertising, promoting, presenting, distributing, or soliciting through the mail, or using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means any material in a manner that reflects the belief or is intended to cause another to believe that the material is or contains a visual depiction of an actual minor engaging in sexually explicit conduct, or an obscene visual depiction of a minor engaging in sexually explicit conduct.

h. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an

image of child pornography that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

C. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing

device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. § 1030(e)(1).

d. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

e. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key

to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

g. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's

computer a particular IP address that is used each time the computer accesses the Internet.

i. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

j. "Peer-to-peer file-sharing" (P2P) is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting searches for files that are currently being shared on another user's computer.

k. "Sexually explicit conduct" applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the

genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

l. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

m. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

6. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

7. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

8. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

9. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

10. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

11. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

12. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic

communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

13. A growing phenomenon on the Internet is peer-to-peer file-sharing (P2P).

14. The latest evolution of P2P software is a program that allows a user to set up his own private P2P network of contacts. File-sharing through this new and publicly available P2P file-sharing program is limited only to other users who have been added to a private list of "friends." A new user is added to a list of friends by request. Acceptance of a friend request will allow that new user to download files from the user who sent the friend request. The new user can then browse the list of files that the other user has made available to download, select desired files from this list, and download the selected files. The downloading of a file occurs through a direct connection between the computer requesting the file and the computer containing the file.

15. One aspect of P2P file sharing is that multiple files may be downloaded in parallel, which permits downloading more than one file at a time.

16. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four sets of numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

17. Third-party software is available to identify the IP address of the P2P computer sending the file. Such software monitors and logs Internet and local network traffic.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

18. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he

or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

19. In order to fully retrieve data from a computer system, the analyst needs all storage devices as well as the

central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

20. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

21. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth

herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

BACKGROUND OF THE INVESTIGATION

22. On May 18, 2009, SA J. Brooke Donahue, using a computer connected to the Internet, launched a publicly available P2P file sharing program from the Innocent Images Unit of the FBI, located in Calverton, Maryland. SA Donahue connected to the file sharing program with a username that he

had obtained through a consenual ID takeover of another subject of a child pornography investigation. SA Donahue queried his network of friends and observed that an individual using the username "Tootyboi" was logged onto the network.

23. SA Donahue browsed Tootyboi's shared folders and observed numerous images depicting child pornography and video files whose titles were indicative of child pornography. SA Donahue selected 21 image and video files of child pornography and began to download these files directly from Tootyboi's computer between 6:36 p.m. Eastern Time and 8:08 p.m. Eastern Time. During the download of these files, SA Donahue used a network monitoring program in order to identify the IP address of Tootyboi's computer. SA Donahue was able to determine that the IP address of Tootyboi's computer was 97.116.10.183.

24. When reviewed, 20 of the 21 downloaded image and video files depicted child pornography. Eight files downloaded that depicted child pornography had the following names and are briefly described:

a. **2633935oat.jpg** - Image depicts a naked prepubescent boy sitting down and exposing his penis

b. **3470244Uxq.jpg** - Image depicts a naked prepubescent boy sitting down with his legs spread and he is holding his penis

c. **Img-e-16.jpg** - Image depicts a prepubescent boy lying down and pulling his shorts down. The boy is holding his penis and is exposing his testicles.

d. **Img-e-19.jpg** - Image depicts an adult male performing oral sex on a prepubescent boy

e. **[webcam] [pre~tod+] [boy] [hc] f4_secondfuck.avi** - Video approximately 4 minutes 25 seconds long depicting a naked prepubescent boy on the lap of an adult male. The adult male is shown touching the boys buttocks with his hand and then anally penetrating the boy with his penis.

f. **5yo Boy Fondles Self 5yo Boy Fondles Self.avi** - Video approximately 2 mintues 6 seconds long Depicting a naked prepubescent boy fondling his penis.

g. **toddler boy - MathewXXX-100_257[[3_4_5_6]]_PC.avi** - video approximately 2 minutes 40 seconds long depicting an adult male performing oral sex on a prepubescent boy. The boy is then shown performing oral sex on the adult male.

h. **2007 Tara 8Yr - arsch fick - h.guenter1@gmx.net.wmv** - video approximately 2 minutes 28 seconds long depicting a naked

prepubescent girl on her knees and being anally penetrated by an adult male.

The images described in a, b, c, and d above and the video described in h above all depict identified victims of child sexual exploitation.

25. Results from an administrative subpoena sent to Qwest on May 29, 2009, for the date and time the files were downloaded revealed that at that day and time the IP address was assigned to the account registered to Gregg A. Larsen, 3536 23rd Ave. S., Minneapolis, Minnesota, 55407.

26. Affiant and SA Donahue have searched various records indices for information regarding Larsen and the username Tootyboi.

a. Public records report accessed through Lexis Nexis, a public records database that can be accessed and searched over the Internet, for Larsen, shows a full name of Gregg Alan Larsen, and a social security account number xxx-xx-2463, date of birth xx/xx/1961, and shows an active address of 3536 23rd Ave. S., Minneapolis, Minnesota 55407. The first five digits of the social security account number, and the month and day of the date of birth has been redacted for the purposes of this affidavit.

b. Minnesota Driver and Vehicle Services records indicate that Larsen currently has a 2006 black Ford Freestyle

sport van bearing license plate PXN984 registered at 3536 23rd Ave. S., Minneapolis, Minnesota.

27. On June 5, 2009, the United States Postal Inspection Service advised that Gregg Larsen is the only person receiving mail at 3536 23rd Ave. S., Minneapolis, Minnesota.

28. On June 5, 2009 , a physical surveillance of 3536 23rd Ave. S., Minneapolis, Minnesota, was conducted. 3536 23rd Avenue South, Minneapolis, Minnesota, is described as a two(2) story residential structure that is light in color with yellow trim. When facing the residence from 23rd Avenue South, the numerals "3536" are clearly visible and are affixed to the residence above the front door. There is a stairway leading to the front door with black railings. On the left railing is a mailbox. The second story front window has dark shutters. There is a detached garage located in an alley directly behind 3536 23rd Avenue South. The detached garage is white with yellow trim and has a green garage door. When facing the garage door, the numerals "3536" are clearly visible and are affixed to the garage to the left side of the garage door. A vehicle bearing Minnesota license plate PXN984 was observed to be parked next to the detached garage. Driver and Vehicle Services records show this vehicle to be registered in the name of Gregg Larsen at this address.

29. On July 1, 2009, I along with other law enforcement executed a search warrant at the residence and recovered items listed in that search warrant. A review of the electronic media reveals that at least one hidden camera was installed in a bathroom in the residence. One of these hidden cameras recorded images of children including one prepubescent boy using the toilet facilities or changing clothes during which the genitals were exposed.

CONCLUSION

29. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that an individual who resides at 3536 23rd Avenue South, Minneapolis, Minnesota, is involved in possession, distribution and production of child pornography. Your affiant respectfully submits that there is probable cause to believe that an individual residing in the residence described above has violated 18 U.S.C. §§ 2252 and 2252A. Additionally, there is probable cause to believe that evidence of criminal offenses, namely, violations of 18 U.S.C. §§ 2252 and 2252A, is located in the residence described above, and this evidence, listed in Attachment B to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

30. Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Further your Affiant sayeth not.

ROBERT J. E. BLACKMORE
Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me

this 2 day of June, 2009.

JEFFREY J. KEYES
United States Magistrate Judge

ATTACHMENT B

1. Internet billing and use records.

2. Records or other items that evidence ownership or use of computer equipment found in the premises to be searched, including, but not limited to, sales receipts, handwritten notes and handwritten notes in computer manuals.

3. Records evidencing occupancy or ownership of the premises to be searched, including, but not limited to, utility and telephone bills, mail envelopes, and/or addressed correspondence.

4. Any and all visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, in any format or media, including, but not limited to, undeveloped photographic film, photographs, magazines, videotapes, slides, and motion picture films.

5. Correspondence, books, ledgers, and/or records pertaining to the possession, receipt, distribution, transportation, or advertisement of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail.

6. Any and all computer passwords and other data security devices designed to restrict access to or hide computer

software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

7. Computer(s) and all related computer equipment, including scanners, peripherals, related instructions in the form of manuals, as well as the software used to operate the computer(s), and any CD-ROMS, zip disks, floppy disks, DVDs, memory cards, other magnetic storage devices and any cameras or video recording devices. The subsequent forensic analysis of these items is to be focused on searching for the items described in paragraphs 1-6 above.